PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-157585
(43)Date of publication of application : 29.05.1992

(51)Int.Cl. G06K 17/00

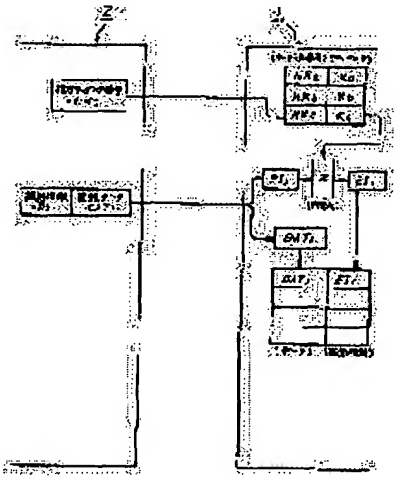
(21)Application number : 02-282035
(22)Date of filing : 22.10.1990

(71)Applicant : TOSHIBA CORP
TOSHIBA INTELIGENT TECHNOL LTD
(72)Inventor : NIIMURA TAKASHI

(54) INFORMATION MANAGEMENT SYSTEM

(57)Abstract:
PURPOSE: To improve data security by disenabling an access to data stored in the data memory of an IC card with any equipment other than a legal host device (host computer).

CONSTITUTION: A second electronic device (host computer) 2 performs data management by assigning identification information to each data. When the second electronic device 2 accesses the storage means of a second electronic device (IC card) 1, when prescribed key data are designated from among several key data Ka to Kc preliminarily stored in the first electronic device 1 by the second electronic device 2, the identification information assigned to each data is coded by using the key data. Each data is assigned with the coded identification information and the access to each data stored in the first electronic device 1 is executed based on the coded identification information. Thus, the security for the data stored in the first electronic device can be improved.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−157585

⑤Int.Cl.⁵	識別記号	庁内整理番号	㊸公開　平成4年(1992)5月29日
G 06 K 17/00	S	6711−5L	
	E	6711−5L	

審査請求　未請求　請求項の数 1　(全8頁)

㊹発明の名称　情報管理方式

㉑特　願　平2−282035
㉒出　願　平2(1990)10月22日

㉗発明者　新村　貴志　神奈川県川崎市幸区柳町70番地　東芝インテリジエントテクノロジ株式会社内
㉑出願人　株式会社東芝　神奈川県川崎市幸区堀川町72番地
㉑出願人　東芝インテリジエントテクノロジ株式会社　神奈川県川崎市幸区柳町70番地
㉔代理人　弁理士　則近　憲佑　外1名

明　細　書

1．発明の名称

情報管理方式

2．請求の範囲

複数のデータと、複数のキーデータとを記憶する記憶手段を有してなる第1の電子装置と、前記第1の電子装置の記憶手段に記憶されているデータの各々に対して識別情報を与える手段を有してなる第2の電子装置とからなり、前記第2の電子装置は前記識別情報に基づいて前記第1の電子装置の記憶手段に記憶されている所定のデータにアクセスするものであって、前記第1の電子装置に設けられた記憶手段中に記憶されている複数のキーデータのうち、前記第2の電子装置により指定されたキーデータを用いて前記識別情報を暗号化する手段を具備してなり、前記第1の電子装置に記憶されている所定のデータへのアクセスは、前記暗号化された識別情報に基づいて行われることを特徴とする情報管理方式。

3．発明の詳細な説明

[発明の目的]

(産業上の利用分野)

本発明は、例えばホストコンピュータ等の上位装置から送信され、不揮発性メモリおよびCPUなどの制御素子を有するIC(集積回路)チップを内蔵したICカードと称される携帯可能記憶媒体に記憶されたデータを管理する情報管理方式に関する。

(従来の技術)

従来、携帯可能なデータ記憶媒体としてEEPROMなどのデータメモリ及びCPUなどの制御素子を有するICチップを内蔵したICカードが考えられている。この種のICカードは内蔵する制御素子によってデータメモリをアクセスし、外部(上位装置)からの要求に応じて必要なデータの入出力を選択的に行うようになっている。このICカードにホストコンピュータから送られたデータはデータメモリ中に順次記憶されていくものである。

ここで前記データメモリ中に記憶されたデー

タに対するアクセスを容易に行う方法として記憶されてい　各データに独自の識別情報を与える方法が考えられている。

識別情報とは例えばデータメモリに記憶された順序を表す数値であり、第１１図に見られるように５つのデータがデータメモリ１０内でＡ、Ｂ、Ｃ、Ｄ、Ｅの順列で格納されている場合、「識別情報２のデータ」とはＢであり、「識別情報４のデータ」とはＤである。今、ホストコンピュータ側から「識別情報２のデータ」の読出命令を受信すると、ＩＣカード内の制御素子はデータメモリ１０内の上位から２番目に格納されているデータ（第１０図の例ではＢ）を読出し、そのデータの内容をホストコンピュータへと送信するものでである。

このような情報管理方式においては、使用者は例えばパスワード等をホストコンピュータを通して入力し、これにより正当な使用者であると認識されればＩＣカードに対してデータの読み書きを行うことができる。

(2)　ところが、前記パスワード照合等の所定の前処理さえ正　に終了していれば、どんなホストコンピュータからでも、ＩＣカード内に記憶されているデータに対するアクセスを容易に行いうるので、データのセキュリティが不充分であった。

（発明が解決しようとする課題）

上述したように従来の識別情報を用いた情報管理方式では、ＩＣカードのデータメモリ内に記憶されたデータに対するアクセスが、どの上位装置からでも簡単に行えるので、データのセキュリティが不充分であるという問題点があった。

そこで本発明は、正当な上位装置（ホストコンピュータ）でなければＩＣカードのデータメモリに記憶されているデータに対してアクセスできないような、データのセキュリティが充分な情報管理方式を提供することを目的とする。

［発明の構成］

（課題を解決するための手段）

上記目的を達成するために、本発明の情報管理方式は、複数のデータと複数のキーデータとを記憶する記憶手段を有してなる第１の電子装置と前記第１の電子装置の記憶手段に記憶されているデータの各々に対して識別情報を与える手段を有してなる第２の電子装置とからなり、前記第２の電子装置は前記識別情報に基づいて前記第１の電子装置の記憶手段に記憶されている所定のデータにアクセスするものであって、前記第１の電子装置に設けられた記憶手段中に記憶されている複数のキーデータのうち、前記第２の電子装置により指定されたキーデータを用いて前記識別情報を暗号化する手段を具備してなり、前記第１の電子装置に記憶されている所定のデータへのアクセスは、前記暗号化された識別情報に基づいて行われることを　徴とする。

（作用）

第２の電子装置（ホストコンピュータ）は各データに識別情報を付してデータ管理を行っている。この第２の電子装置から第１の電子装置（ＩＣカード）の記憶手段に対してアクセスを行う場合には、まず第２の電子装置は第１の電子装置にあらかじめ記憶されている複数のキーデータの中から、所定のキーデータを指定する。次に、このキーデータを用いて、各データに与えられている識別情報が暗号化される。そして、各データには、この暗号化された識別情報が付与され、第１の電子装置に記憶された各データへのアクセスは、暗号化された識別情報に基づいて行われる。

（実施例）

以下、本発明をＩＣカードとホストコンピュータとからなるシステムに適用した一実施例を、図面を参照して説明する。

第３図はＩＣカード１とホストコンピュータ２とからなるシステムの構成例を示すものである。このＩＣカード１は制御部としての制御素子３（例えばＣＰＵ）を含む。そして、この制御素子３によりデータメモリ４、プログラムメモリ５及びコンタクト部６が制御されている。このうち、データメモリ４は各種データの記憶に使用され、例えばＥＥＰＲＯＭで構成されている。また、プログラムメモリ５は、例えばマスクＲＯＭで構成

されており、制御素子３の制御プログラムなどを記　するものである。コンタクト部６は、後述するホストコンピュータ２のカードリーダライタ８との電気的接触を得るためのものである。ここで破線内の部分、制御素子１５、データメモリ１６、プログラムメモリ１７は１つのＩＣチップで構成されてＩＣカード本体内に埋設されている。さて、ホストコンピュータ２側も、例えばＣＰＵからなる制御部７を有する。そして、この制御部８によって、カードリーダライタ８、キーボード９、ＣＲＴディスプレイ１０が制御されている。このうち、カードリーダライタ８は前述したＩＣカード１に対してデータの書込み、読出し等を行うものである。また、キーボード９は例えば、制御部７に対する指示を入力したり、ＩＣカード１に書込むデータを入力したりするための入力手段である。ＣＲＴディスプレイ１０は、カードリーダライタ８を通して読出されたＩＣカード１のデータメモリ４の内容を表示したり、何らかのエラーが発生した場合にエラーメッセージを表示したりするための表示手段である。

ここで、前記ＩＣカード１のプログラムメモリ５内には、後述する「識別情報」を暗号化するのに使用される「キーデータ」があらかじめ複数個記憶されている。これら「キーデータ」の各々には、それぞれ独自の「キーデータ番号」が付与されており、「キーデータ」と「キーデータ　号」とは対応づけられて記憶されている。また、ホストコンピュータ２の制御部７は、データをＩＣカード１に対して書込む際、各データに独自の「識別情報」を付与し、この「識別情報」に基いて各データを管理している。ここで、この「識別情報」は各データと一対一に対応している。

いま、ホストコンピュータ２からＩＣカード１に対してデータの書込みを行う場合の動作について第１図及び第２図を用いて説明する。まず、オペレータがホストコンピュータ２に設けられたキーボード６を通じてパスワードを入力し（Ｓｔｅｐ１）、制御部７はこのパスワードが正当なものかどうかを判断する（Ｓｔｅｐ２）。正当なパスワードが入力されると、ＩＣカード１に対するアクセスが許可される（Ｓｔｅｐ３）。ここで、正当でないパスワードが入力されたなら、その旨のエラー表示がＣＲＴディスプレイ１０上に表示され（Ｓｔｅｐ４）、例えばもう一度パスワードの入力を促す。次に制御部７はＩＣカード１のプログラムメモリ５中に記憶されているキーデータのキーデータ番号の中から、所定のキーデータ番号ＮＫｃを指定する（Ｓｔｅｐ５）。ここで、どのキーデータ番号を指定するかはホストコンピュータ２の制御部７によって予め定められている。続いて、このキーデータ番号ＮＫｃに対応しているキーデータＫｃがプログラムメモリ５中で検索される（Ｓｔｅｐ６）。そして指定されたキーデータ番号ＮＫｃが存在しない場合は、その旨のエラー表示をＣＲＴディスプレイ１０上に表示し（Ｓｔｅｐ７）処理を終了する。

以上の処理が正常に終了す　とホストコンピュータ２は　込みを行うデータＤＡＴ１に与えられている識別情報ＰＩ１と書込みを行うデータＤＡＴ１とをＩＣカード１に対して送信する（Ｓｔｅｐ８）。次にホストコンピュータ２から識別情報ＰＩ１を受け取ったＩＣカード１では、先にホストコンピュータ２によって指定されたキーデータＫｃを用いて制御素子３が前記識別情報ＰＩ１を暗号化し、暗号化識別情報ＥＩ１を生成する処理が行われる（Ｓｔｅｐ９）。続いてＩＣカード１のデータメモリ４内に暗号化識別情報ＥＩ１と、これに対応するデータＤＡＴ１が記録される（Ｓｔｅｐ１０）。このとき、データメモリ４内では第４図に示されるようにデータは暗号化識別情報に連続して記憶され「暗号化識別情報、データ、暗号化識別情報、データ、…」のように隙間なく詰めて記憶されている。更にデータの先頭には該データのデータ長を表す情報（図示しない）が付加されて記憶される。

次に以上のような動作によって書込まれたデータを読出す処理について第５図及び第６図を用いて説明する。

ここで、データの読出し処理において、パス

(4)

ワード入力から指定キーデータの検索までの動作（Ｓｔｅｐ１からＳｔｅｐ７までの動作）は先に説明したデータの書込み処理における動作と共通であるので、説明を省略する。さて、次に、オペレータは読出しを行うデータＤＡＴ１の識別情報ＰＩＤをキーボード９等からの入力により指定する（Ｓｔｅｐ８）。続いて、先に指定されたキーデータＫｃを用いて、ホストコンピュータ２側の制御部７が、前記識別情報ＰＩＤを暗号化し、暗号化識別情報ＥＩＤが生成される（Ｓｔｅｐ９）。そして、この暗号化された識別情報ＥＩＤがＩＣカード１に対して送信される（Ｓｔｅｐ１０）。一方ＩＣカード１側では、制御素子３がデータメモリ４内の暗号化識別情報を次々と検索してゆき該当する暗号化識別情報がデータメモリ４内に存在するかどうかを判断する（Ｓｔｅｐ１１）。ここで、該当する暗号化識別情報ＥＩＤがデータメモリ４内に存在する場合、該データメモリ４内で、該暗号化識別情報ＥＩＤの直後に格納されているデータＤＡＴ１の読出しが行われ（Ｓｔｅｐ１２）、このデータＤ.ＡＴ１がホストコンピュータ２側に送信される（Ｓｔｅｐ１３）。前記Ｓｔｅｐ１１において、ホストコンピュータ２から送信されてきた暗号化識別情報ＥＩＤがＩＣカード１のデータメモリ４内に存在しない場合は、「該当するデータは存在しない」旨のエラーメッセージをホストコンピュータ２に送信して（Ｓｔｅｐ１４）、読出し処理を終了する。

次に、データメモリ４内の様子を参照して、データの読出し動作について説明する。今、第７図に見られるように５つのデータＤＡＴ１、ＤＡＴ２、ＤＡＴ３、ＤＡＴ４、ＤＡＴ５がデータメモリ４中に記憶されており、これらデータには暗号化識別情報ＥＩ１、ＥＩ２、ＥＩ３、ＥＩ４、ＥＩ５がそれぞれ与えられているものとする。ここで、暗号化識別情報ＥＩ３のデータＤＡＴ３を消去する処理について説明する。制御素子３はデータメモリ４内の上から順に暗号化識別情報を検索していく。まず、最初に制御素子３は暗号化識別情報ＥＩ１を認識するが、処理対象の暗号化識別情報ＥＩ３ではないので、次の暗号化識別情報を検索する。このとき、暗号化識別情報ＥＩ１のデータＤＡＴ１のデータ長を参照して、該データ長分ジャンプすることによって、次の暗号化識別情報を認識する。このようにして制御素子３はデータメモリ４内で次々と暗号化識別情報を検索していく。そして処理対象データＤＡＴ３の暗号化識別情報ＥＩ３が認識されるとそれに連続して格納されているデータＤＡＴ３に対して消去する処理を行う。このとき、制御素子３はデータＤＡＴ３のデータ長を参照して、データＤＡＴ３自体を消去するとともに、このデータＤＡＴ３に付与されていた暗号化識別情報ＥＩ３も同時に消去する。そしてデータＤＡＴ３及び暗号化識別情報ＥＩ３が格納されていた領域は未使用領域となる。こうして、データＤＡＴ３が消去された後のデータメモリ４内の様子を第８図に示す。

いま、ホストコンピュータ２からＩＣカード１に対して識別情報ＰＩ６とデータＤＡＴ６とが送信されてきたとする。この識別情報ＰＩ６は前述した動作により、暗号化識別情報ＥＩ６となる。一方、制御素子３は、データメモリ４中を先頭から検索し、最初に存在する未使用領域に暗号化識別情報ＥＩ６及びデータＤＡＴ６とを格納する。ここで、最初に存在する未使用領域に暗号化識別情報ＥＩ６及びデータＤＡＴ６が格納しきれなかった場合、制御素子３は例えば第９図に見られるように、次に存在する未使用領域を検索し、データＤＡＴ６を分割して格納する。このとき、分割されたデータＤＡＴ６－１の末尾には、これに連続するデータＤＡＴ６－２がデータメモリ４内のどこに格納されたかを表す連続情報１１が付加される。この連続情報１１は例えばデータＤＡＴ６－２の先頭アドレスが記録されている。

また、データメモリ４中にすでに格納されているデータ群の末尾に新たなデータを追加記録する場合について説明する。例えば第７図に示すようにデータメモリ４内に５つのデータＤＡＴ１、ＤＡＴ２、ＤＡＴ３、ＤＡＴ４、ＤＡＴ５が格納されており、それぞれのデータの暗号化識別情報

がＥＩ１、ＥＩ２、ＥＩ３、ＥＩ４、ＥＩ５であるとする。今、新たなデータとしてデータＤＡＴ６を追加格納する。このデータＤＡＴ６の識別情報ＰＩ６は暗号化されて暗号化識別情報ＥＩ６となる。そして、制御素子１がデータメモリ４内の未使用領域を検索して、検索された未使用領域に暗号化識別情報ＥＩ６ならびにデータＤＡＴ６を格納する。このときのデータメモリ４内の様子を第１０図に示す。データＤＡＴ６を格納するための未使用領域がデータメモリ４内に存在しなかった場合は、「メモリがいっぱいである」旨のメッセージをホストコンピュータ２に送信して処理を停止する。

以上詳述したように本実施例では、ホストコンピュータによって指定されたキーデータによってデータの識別情報を暗号化し、この暗号化された識別情報を用いてＩＣカードに記憶されるデータの管理が行われる。このため、キーデータを正しく指定できないホストコンピュータからは、ＩＣカードに記憶されているデータの正しい識別情報を指定することができない。即ち、正当なホストコンピュータしか、ＩＣカードに記憶されているデータに対してのアクセスを行いえないので、データのセキュリティが高められる。更に、データ自身を暗号化することなく、識別情報のみを暗号化するので、制御素子（ＣＰＵ）の負担を小さくできる。

また、ＩＣカードに記憶される各データに与えられる暗号化識別情報は絶対的な値であり、それぞれが独立している。そのため、一度、暗号化識別情報が与えられると該暗号化識別情報とデータとの対応が変化しないので、データ管理を容易に行うことができる。

なお、以上説明した実施例では、データ書込時にはＩＣカード１側で識別情報の暗号化を行い、既にＩＣカード１のデータメモリ４内に格納されているデータに対して処理を行う場合（以下データ処理時と称する）には、ホストコンピュータ２側で、識別情報の暗号化を行う。ここで、データを書込む際にはホストコンピュータ２側で識別情報の暗号化を行い、書込まれたデータを処理する際にはＩＣカード１側で識別情報の暗号化を行うものであってもよい。また、データ書込時においても、データ処理時においても、識別情報の暗号化をホストコンピュータ２側で行うものであってもよい。更に、また、データ書込時においても、データ処理時においても、識別情報の暗号化をＩＣカード１側で行うものであってもよい。

また、本実施例中では、キーデータ番号並びにキーデータは、予めＩＣカードのプログラムメモリ５中に格納されているものであったが、キーデータ番号並びにキーデータがデータメモリ４中のある領域に格納されるものであってもよい。

【発明の効果】

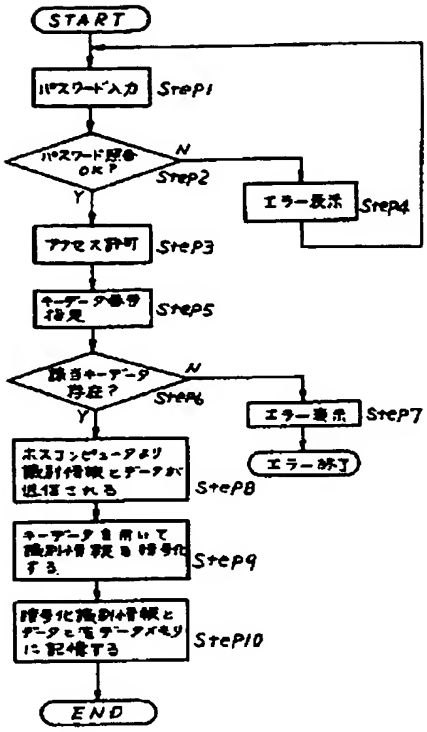
上述したように、本発明の情報管理方式によれば、正しいキーデータを指定することのできる正当な第２の電子装置（ホストコンピュータ）のみによってしか第１の電子装置（ＩＣカード）に格納されてい　データに対するアクセスは行いえず、第１の電子装置に格納されているデータのセキュリティが高められる。

４．図面の簡単な説明

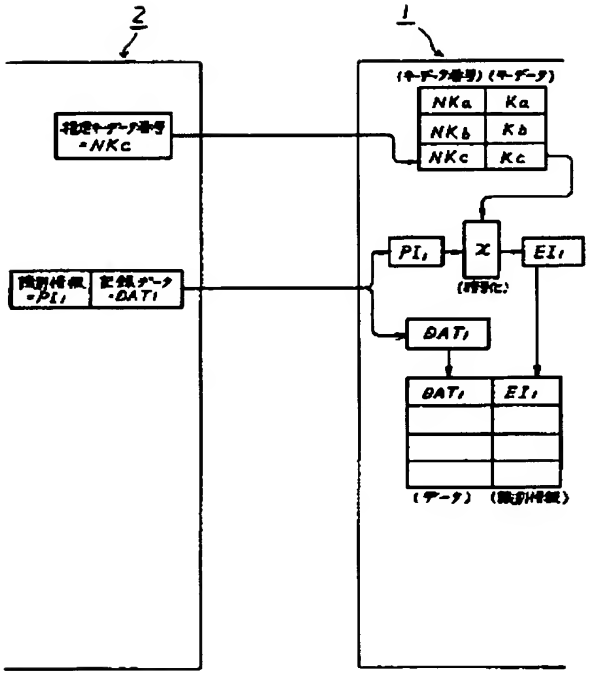
第１図乃至第９図は本実施例を説明するためのもので、第１図はデータ書込み処理を行う場合のフローチャート、第２図はデータ書込み処理を行う場合のＩＣカードとホストコンピュータ間のデータの授受を説明するための図、第３図はデータメモリ中の様子を説明するための図、第４図はデータ読出し処理を行う場合のフローチャート、第５図はデータ読出し処理を行う場合のＩＣカードとホストコンピュータ間のデータの授受を説明するための図、第６図はデータメモリ内の記憶データ例を示す図、第７図はデータＤＡＴ３を消去した後のデーメタモリ内の様子を示す図、第８図はデータメモリ中の未使用領域に新しいデータを挿入した場合のデータメモリ内の様子を示す図、第９図はデータを分割格納したときのデータメモリ内の様子を示す図、第１０図は新たなデータを追加格納したときのデータメモリ内の様子を示す図、第１１図は従来例を説明するための図である。

1 … ＩＣカード
2 … ホストコンピュータ
3 … 制御素子
4 … データメモリ
5 … プログラムメモリ

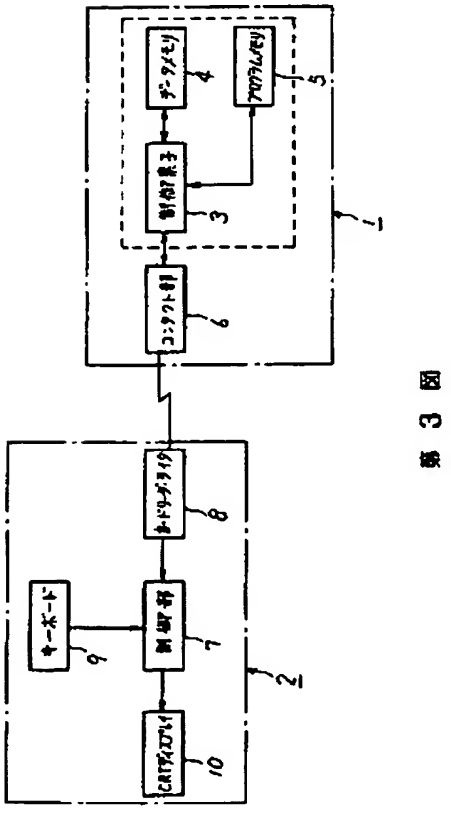
代理人　弁理士　則　近　憲　佑
同　山　下　一



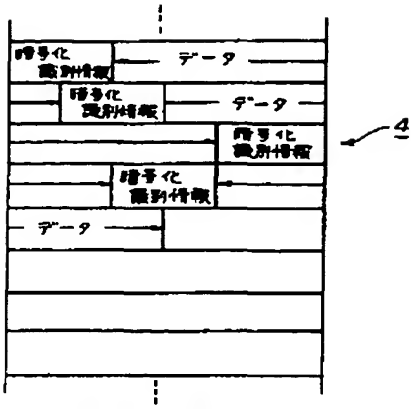
第 1 図



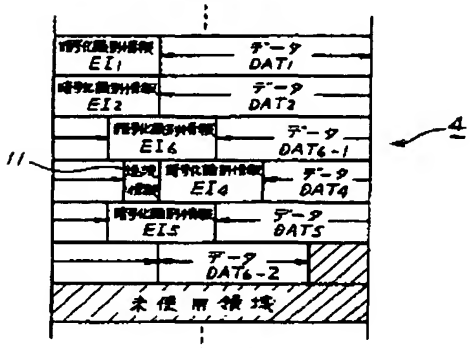
第 2 図



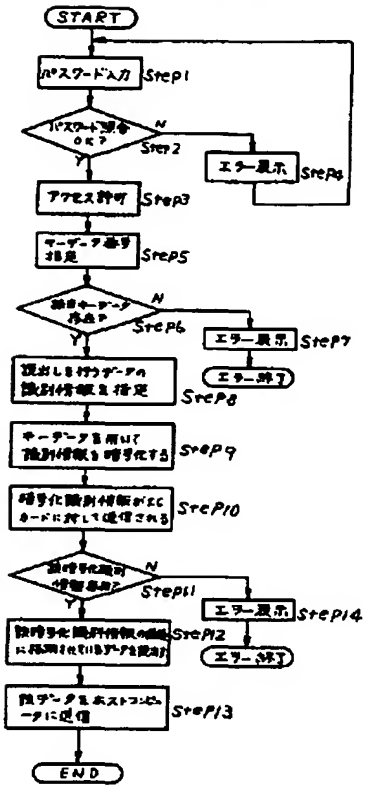
第 3 図



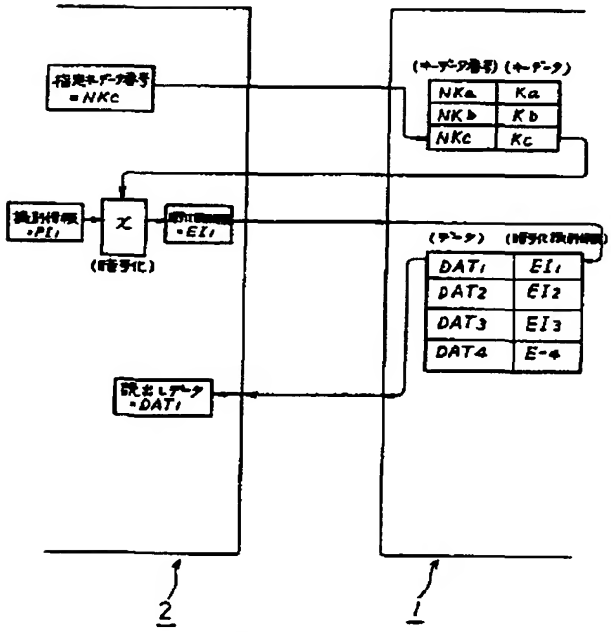
第 4 図



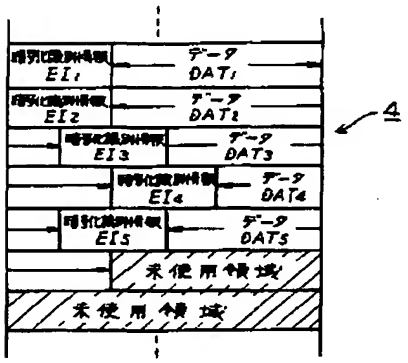
第 9 図



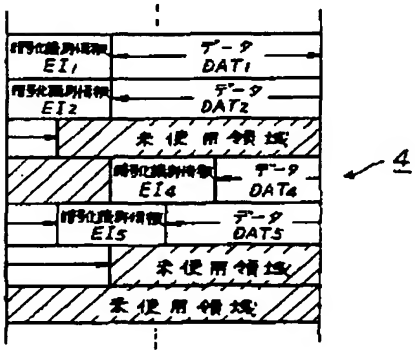
第 5 図



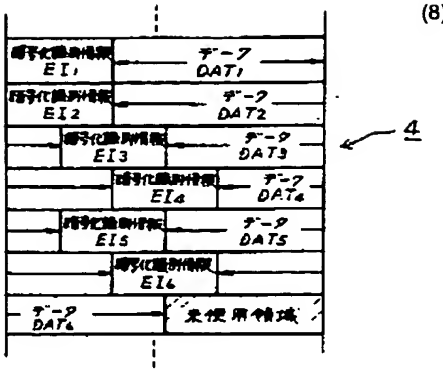
第 6 図



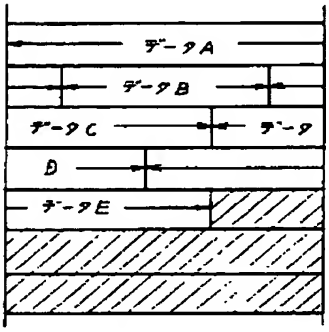
第 7 図



第 8 図


EI1
データ DAT1
EI2
データ DAT2
EI3
データ DAT3
4
EI4
データ DAT4
EI5
データ DAT5
EI6
データ DAT6
未使用領域

第 10 図


データA
データB
データC
データ
D
データE

第 11 図